

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 1. (Currently amended) A system comprising:
2 a controller module comprising instructions for controlling a first
3 component; and
4 a second component with a security system that interacts with the
5 controller module to implement a security protocol before the a second component
6 can control the first component based on executing the instructions in the
7 controller module, wherein the controller module provides secure control of
8 communications between the first component and the second component, and
9 wherein the security system decrypts an encrypted controller module to perform a
10 portion of the security protocol, the second component controls the first
11 component based upon the execution of the instructions in the controller module.

1 2. (Original) The system as set forth in claim 1 wherein a portion of the
2 instructions in the controller module comprises authentication instructions which
3 when executed by the second component cause the second component to send
4 authentication information to the first component to perform a portion of the
5 security protocol.

1 3. (Original) The system as set forth in claim 2 wherein the
2 authentication information is associated with an operator of the second
3 component, the first component authenticates the operator using the

4 authentication information to perform another portion of the security
5 protocol.

1 4. (Original) The system as set forth in claim 2 wherein the first
2 component authenticates the second component using the authentication
3 information to perform another portion of the security protocol, wherein upon
4 unsuccessful authentication the first component rejects messages from the second
5 component and upon successful authentication the first component accepts the
6 messages from the second component, the messages being associated with
7 controlling the first component.

1 5. (Original) The system as set forth in claim 2 wherein the first
2 component authenticates each of a plurality of messages received from the second
3 component, the messages being associated with controlling the first component,
4 wherein upon unsuccessful authentication of at least one of the messages the first
5 component rejects the at least one message and upon successful authentication of
6 another at least one of the messages the first component accepts the other at least
7 one message from the second component.

1 6 (Canceled).

1 | 7. (Currently amended) The system as set forth in claim 1 ~~claim 6~~ wherein
2 the security system uses a cryptographic key associated with one of the first
3 component, the second component and a third component to decrypt the encrypted
4 controller module.

1 8. (Original) The system as set forth in claim 1 wherein the security
2 system authenticates the controller module using at least one of a digital

3 certificate, a public key and a shared secret to perform a portion of the
4 security protocol.

1 9. (Original) The system as set forth in claim 1 wherein the security system
2 rejects the controller module upon determining that a cryptographic signature
3 associated with the controller module is not associated with a trusted component
4 to perform a portion of the security protocol.

1 10. (Original) The system as set forth in claim 1 wherein the controller
2 module is encrypted using a cryptographic key from one of the first component,
3 the second component and a third component.

1 11. (Original) The system as set forth in claim 1 wherein the controller
2 module comprises a cryptographic signature associated with at least one of the
3 first component and one or more third components.

1 12. (Currently amended) A method comprising:
2 providing a controller module comprising instructions for
3 controlling a first component; and
4 interacting with the controller module to implement a security protocol
5 before a second component can control the first component based on executing
6 the instructions in the controller module, wherein the controller module provides
7 secure control of communications between the first component and the second
8 component,
9 wherein the interacting with the controller module to implement the
10 security protocol further comprises:
11 decrypting an encrypted controller module to perform a
12 portion of the security protocol, and

13 | controlling the first component based upon the execution of
14 | the instructions in the controller module.

1 13. (Original) The method as set forth in claim 12 wherein the interacting
2 with the controller module to implement the security protocol further comprises:
3 executing a portion of the instructions in the controller module that
4 comprises authentication instructions;
5 sending authentication information from the second component to the first
6 component to perform a portion of the security protocol based on the executed
7 authentication instructions.

1 14. (Original) The method as set forth in claim 13 further comprising
2 authenticating an operator of the second component using the authentication
3 information to perform another portion of the security protocol.

1 15. (Original) The method as set forth in claim 13 further comprising:
2 authenticating the second component using the authentication
3 information to perform another portion of the security protocol; and
4 rejecting messages from the second component upon unsuccessful
5 authentication and accepting the messages from the second component upon
6 successful authentication, the messages associated with controlling the first
7 component.

1 16. (Original) The method as set forth in claim 13 further comprising:
2 authenticating each of a plurality of messages from the second
3 component, the messages associated with controlling the first component;
4 and

5 rejecting at least one of the messages from the second component upon
6 unsuccessful authentication of the at least one message and accepting another
7 at least one of the messages upon successful authentication of the other at
8 least one message.

1 17 (Canceled).

1 18. (Currently amended) The method as set forth in claim 12~~claim 17~~
2 further comprising using a cryptographic key associated with one of the first
3 component, the second component and a third component to decrypt the encrypted
4 controller module.

1 19. (Original) The method as set forth in claim 12 further comprising
2 authenticating the controller module using at least one of a digital certificate, a
3 public key and a shared secret to perform a portion of the security protocol.

1 20. (Original) The method as set forth in claim 12 further comprising
2 rejecting the controller module upon determining that a cryptographic signature
3 associated with the controller module is not associated with a trusted component
4 to perform a portion of the security protocol.

1 21. (Original) The method as set forth in claim 12 further comprising
2 encrypting the controller module using a cryptographic key from one of the first
3 component, the second component and a third component.

1 22. (Original) The method as set forth in claim 12 wherein the controller
2 module comprises a cryptographic signature associated with at least one of the
3 first component and one or more third components.

1 23. (Currently amended) A computer-readable medium having stored
2 thereon instructions, which when executed by at least one processor, causes the
3 processor to perform:
4 providing a controller module comprising instructions for
5 controlling a first component; and
6 interacting with the controller module to implement a security
7 protocol before a second component can control the first component based on
8 executing the instructions in the controller module, wherein the controller
9 module provides secure control of communications between the first
10 component and the second component;
11 wherein the interacting with the controller module to implement the
12 security protocol further comprises:
13 decrypting an encrypted controller module to perform a
14 portion of the security protocol, and
15 controlling the first component based upon the
16 execution of the instructions in the controller module.

1 24. (Original) The medium as set forth in claim 23 wherein the interacting
2 with the controller module to implement the security protocol further comprises:
3 executing a portion of the instructions in the controller module that
4 comprises authentication instructions;
5 sending authentication information from the second component to the first
6 component to perform a portion of the security protocol based on the executed
7 authentication instructions.

1 25. (Original) The medium as set forth in claim 24 further comprising
2 authenticating an operator of the second component using the authentication
3 information to perform another portion of the security protocol.

1 26. (Original) The medium as set forth in claim 24 further comprising:
2 authenticating the second component using the authentication
3 information to perform another portion of the security protocol; and
4 rejecting messages from the second component upon unsuccessful
5 authentication and accepting the messages from the second component upon
6 successful authentication, the messages associated with controlling the first
7 component.

1 27. (Original) The medium as set forth in claim 24 further comprising:
2 authenticating each of a plurality of messages from the second
3 component, the messages associated with controlling the first component;
4 and
5 rejecting at least one of the messages from the second component upon
6 unsuccessful authentication of the at least one message and accepting another at
7 least one of the messages upon successful authentication of the other at least one
8 message.

1 28 (Canceled).

1 | 29. (Currently amended) The medium as set forth in claim 23~~claim 28~~
2 further comprising using a cryptographic key associated with one of the first
3 component, the second component and a third component to decrypt the
4 encrypted controller module.

1 30. (Original) The medium as set forth in claim 23 further comprising
2 authenticating the controller module using at least one of a digital certificate, a
3 public key and a shared secret to perform a portion of the security protocol.

1 31. (Original) The medium as set forth in claim 23 further comprising
2 rejecting the controller module upon determining that a cryptographic signature
3 associated with the controller module is not associated with a trusted component
4 to perform a portion of the security protocol.

1 32. (Original) The medium as set forth in claim 23 further comprising
2 encrypting the controller module using a cryptographic key from one of the first
3 component, the second component and a third component.

1 33. (Original) The medium as set forth in claim 23 wherein the controller
2 module comprises a cryptographic signature associated with at least one of the
3 first component and one or more third components.